Master Eii - TD de Cryptographie

Fiche 1

Recherche de solutions dans l'ensemble des entiers relatifs

Équation ax + by = 1 où a et b sont premiers entre eux

Le théorème de Bachet-Bézout affirme que cette équation admet toujours au moins une solution. La première étape de la résolution consiste à trouver une solution particulière, c'est-à-dire un couple d'entiers relatifs (x_0, y_0) vérifiant : $ax_0 + by_0 = 1$. L'algorithme d'Euclide étendu permet d'en exhiber une.

Ensemble des solutions — Une solution particulière (x_0, y_0) étant connue, l'ensemble des solutions est formé des couples $(x_0 + bk, y_0 - ak)$ où k est un entier relatif quelconque.

Équation ax + by = c où a et b sont premiers entre eux

Une solution particulière peut être trouvée en multipliant par c une solution particulière de l'équation ax + by = 1. En effet, si (x_0, y_0) vérifie $ax_0 + by_0 = 1$ alors $ax_0c + by_0c = c$, le couple (x_0c, y_0c) est alors solution de l'équation ax + by = c. Un raisonnement analogue au précédent permet de trouver l'ensemble des solutions.

Ensemble des solutions — Une solution particulière (x_1, y_1) étant connue, l'ensemble des solutions est formé des couples $(x_1 + bk, y_1 - ak)$ où k est un entier relatif quelconque.

Cas général

On appelle d le pgcd de a et de b.

Si c n'est pas un multiple de d — L'équation n'a pas de solution.

Si c est un multiple de d — L'équation admet toujours des solutions. Une solution particulière (x_1, y_1) étant connue, l'ensemble des solutions est formé des couples où k est un entier relatif quelconque.

$$\left(x_1 + \frac{bk}{d}; y_1 - \frac{ak}{d}\right)$$

1. Calculer le PGCD de 11200 et 15092 par la méthode d'Euclide.

2. En déduire une identité de Bezout entre 11200 et 15092.

3. En déduire l'ensemble des solutions de chacune des 2 équations diophantiennes linéaires suivantes :

11200 x + 15092 y = 252 11200 x + 15092 y = 90

Master Eii - TD de Cryptographie

Fiche 2

Définition et exemple de l'indicatrice d'Euler

- L'**indicateur d'Euler** φ est la fonction de l'ensemble $\mathbb{N}^*$ des entiers strictement positifs dans lui-même qui à *n* associe le nombre d'entiers strictement positifs inférieurs ou égaux à *n* et premiers avec *n*.

Plus formellement :

$$\begin{array}{rccl} \varphi & : & \mathbb{N}^* & \longrightarrow & \mathbb{N}^* \\ & & n & \longmapsto & \mathrm{card}(\{m \in \mathbb{N}^* \mid m \leq n \text{ et } m \text{ premier avec } n\}). \end{array}$$

Si u *et* v *sont deux entiers strictement positifs et premiers entre eux, alors φ(*u.v*)=φ(*u*).φ(*v*)*

La valeur de l'indicatrice d'Euler s'obtient par l'expression de *n* donnée par le théorème fondamental de l'arithmétique :

$$\text{Si} \quad n = \prod_{i=1}^{q} p_i^{k_i} \quad \text{alors} \quad \varphi(n) = \prod_{i=1}^{q} (p_i - 1) p_i^{k_i - 1} = n \prod_{i=1}^{q} \left(1 - \frac{1}{p_i}\right)$$

Dans la formule, p_i désigne un nombre premier et k_i un entier strictement positif.

Le petit théorème de Fermat est généralisé par le théorème d'Euler : pour tout entier naturel non nul *n* et tout entier *a* premier avec *n*, on a :

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

où φ(*n*) désigne la fonction φ d'Euler comptant les entiers entre 1 et *n* qui sont premiers avec *n*.

Si *n* est un nombre premier, alors φ(*n*) = *n* - 1.

1. Calculer la décomposition de 97300 en facteur premiers.

2. En déduire que φ (97300) (=quantité de nombres premiers avec 97300 entre 1 et 97300).

3. Utiliser le petit théorème de Fermat pour trouver un exposant k tel que $3^k = 1 \bmod 97300$.

4. En déduire la valeur de $3^{165603} \bmod 97300$.

Master Eii - TD de Cryptographie

Fiche REVISIONS

Exercice 1

1. Calculer le PGCD de 16558 et 10506 par la méthode d'Euclide.

2. En déduire une identité de Bezout entre 16558 et 10506.

3. En déduire l'ensembles des solutions de chacune des 2 équations diophantiennes linéaires suivantes :

$16558\,x + 10506\,y = 126$ $\qquad$ $16558\,x + 10506\,y = 544$

Exercice 2

1. Calculer la décomposition de 76200 en facteur premiers.

2. En déduire que φ (76200) (=quantité de nombres premiers avec 76200 entre 1 et 76200).

3. Utiliser le petit théorème de Fermat pour trouver un exposant k tel que $7^k = 1 \bmod 76200$.

4. En déduire la valeur de $7^{100802} \bmod 76200$.

Exercice 3

1. Trouver toutes les solutions $(x, y) \in Z^2$ de l'´equation : $2\,x + 5\,y = 37$

2. Pour payer une somme de 37 Euros on ne dispose que de pièces de 2 Euros et de billets de 5 Euros. Soit x le nombre de pièces et y le nombres de billets nécessaires pour payer, alors x + y est le nombre total de pièces et billets utilisés. Quelle est la valeur minimale de x + y ? Que valent x et y dans ce cas ?

Exercice 4

1. Donner la décomposition en facteurs premiers des nombres suivants : 420, 39732, 15543.

2. Calculer φ (420), φ (39732), φ (15543).

3. Vérifier que si n est le numéro de votre jour de naissance alors $P(n) = 2n^2 - 20n + 79$ est un nombre premier.

4. Est-ce que P(n) est premier pour tout $n \in N$?